

Entanglement Purification with the Exchange Interaction

Adrian Auer* and Guido Burkard

Department of Physics, University of Konstanz, D-78457 Konstanz, Germany

Entanglement purification allows the creation of qubit pairs of arbitrarily high fidelity with respect to a maximally entangled state, starting from a larger number of low-fidelity pairs. Purification requires quantum memory, a role for which electron spins are well suited. However, using existing recurrence protocols involving symmetric local two-qubit operations for spin qubits turns out to be rather unpractical. We present an efficient purification protocol requiring only a single pulsed Heisenberg- or XY-type exchange interaction between two qubit pairs. In contrast to known protocols, we allow for asymmetric bilateral two-qubit operations where the two communication parties operate differently on their qubits. In the optimal version of our protocol, the local two-qubit interactions in the case of Heisenberg exchange correspond to the $\sqrt{\text{SWAP}}$ gate and its inverse.

PACS numbers: 03.65.Ud, 03.67.Hk, 03.67.Ac, 85.75.-d

Introduction. Many quantum communication (QC) protocols [1] rely on the faultless distribution of maximally entangled two-qubit states. Well-known examples are quantum teleportation [2] and quantum dense coding [3], while quantum key distribution is possible without [4] or with entanglement [5]. Due to imperfect sources and the inevitable interaction of the entangled particles with their environment, however, the degree of entanglement decreases, and the security or feasibility of the mentioned QC protocols cannot be guaranteed. In the realistic scenario of noisy channels the entanglement can be restored using the method of *entanglement purification*, also known as *quantum privacy amplification* [6–8].

The idea is to use two or more imperfectly entangled qubit pairs to purify one of them with respect to a maximally entangled state. The principle of entanglement purification is specifically harnessed as a building block of quantum repeaters [9, 10]. In large-scale QC networks [11], long-distance entanglement between stationary qubits, acting as quantum memory [12], has to be established, and photons are typically used to transfer quantum information between them. Due to lossy communication channels, e.g. optical fibers, photons can be lost or decohere, which impedes the entanglement production between remote nodes. The working principle of the quantum repeater established in [9, 10] is to divide the distance between the network nodes into smaller segments, create entangled states between them, purify these states individually, and finally connect them via entanglement swapping [13].

A promising candidate for the realization of the stationary qubits are electron spins, e.g. in semiconductor quantum dots (QDs) [14]. Due to their long coherence times of several μs [15] and their complete controllability by electrical [16] or optical [17] means, spin qubits have considerable potential for quantum computation or as quantum memories. However, the original purification proposals [6, 7] make use of a bilaterally applied controlled-NOT (CNOT) operation. In the case of spin qubits in tunnel-coupled QDs, the interaction is

of Heisenberg-exchange type, which needs to be supplemented with single-spin rotations to produce a CNOT gate [14]. It would therefore be advantageous to perform entanglement purification directly using the exchange interaction. In this paper, we present a simple purification protocol based solely on the one-time activation of a Heisenberg interaction leading to the $\sqrt{\text{SWAP}}$ gate. Following the same approach, we also find a similar result for qubits coupled via a XY-type interaction, which happens to be the interaction between superconducting qubits [18] as well as between optically coupled spin qubits [19].

Earlier works have demonstrated purification schemes for spin qubits e.g. by replacing the CNOT in the bilateral operation by the gate sequence that uses two-qubit gates directly generated from the interaction Hamiltonian [20], requiring additional single-qubit operations. Other procedures use three input pairs [21–23] or specifically work for two-spin singlet-triplet qubits [24]. Our proposal works with two input pairs of spin 1/2 qubits and only requires a single two-qubit interaction. In comparison with existing protocols, we achieve an advantage by allowing for *different* two-qubit manipulations locally in the bilateral operation.

Entanglement Purification. A basis of the two-qubit Hilbert space is given by the maximally entangled Bell states $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, where $\{|0\rangle, |1\rangle\}$ is the single-qubit logical basis of the sharing parties, conventionally named Alice and Bob, and we call the overlap of an arbitrary state ρ with the desired entangled state $|\Phi^+\rangle$ its *fidelity* $F \equiv \langle \Phi^+ | \rho | \Phi^+ \rangle$. Recurrence protocols work on two or more qubit pairs of low fidelity as input to create a single qubit pair with higher fidelity as output using only local unitary operations, measurements, and two-way communication of the measurement results via a classical channel. Having initially many copies of the low-fidelity pairs and running the purification protocol iteratively on the output pairs with higher fidelity, one can achieve fidelities arbitrarily close to $F = 1$ and thus obtain a maximally entangled state.

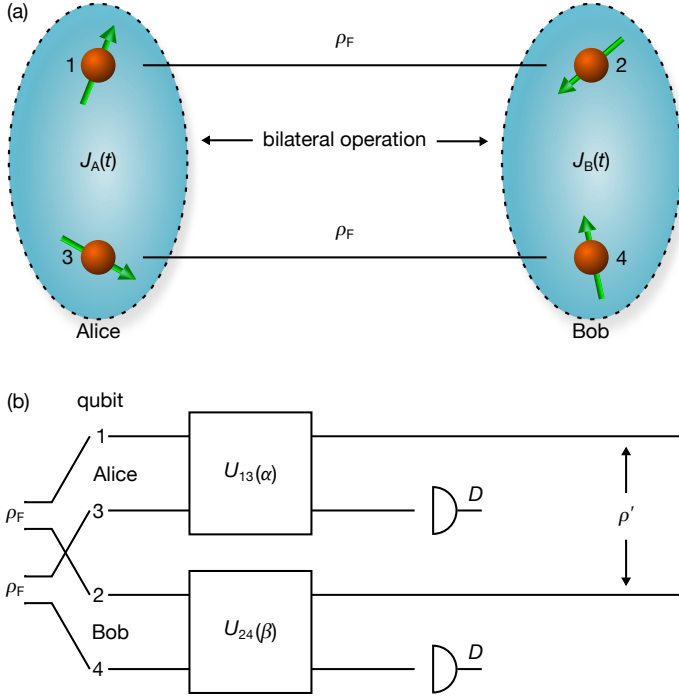


FIG. 1. (a) Alice and Bob share two imperfectly entangled qubit pairs ρ_F and locally apply different unitary operations generated by the exchange couplings J_A and J_B . (b) Circuit diagram of the protocol explained in the main text, where unitary operations with different pulse areas α and β are applied. After the detection (D) of qubits 3 and 4, Alice and Bob are left with the two-qubit state ρ' .

The protocol of Bennett *et al.* [6] (BBPSSW) requires two copies of the state ρ_F (Fig. 1),

$$\rho_F = F|\Phi^+\rangle\langle\Phi^+| + \frac{1-F}{3}(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|), \quad (1)$$

which can be generated from an arbitrary two-qubit state having overlap F with the rotationally invariant singlet state $|\Psi^-\rangle$ by a *twirl* operation [6, 25] that retains the singlet component, equalizes the triplet components and removes all off-diagonal elements, thus creating a so-called Werner state [26], followed by a π rotation about the y axis on the Bloch sphere by one of the sharing parties, hence interchanging the $|\Psi^-\rangle$ and $|\Phi^+\rangle$ components. Next, Alice and Bob each perform a CNOT gate between the two qubits they hold, respectively, where the qubits of the first (second) pair serve as source (target) bit and the target bit is flipped if the source qubit is in state $|1\rangle$, i.e., $|00\rangle \mapsto |00\rangle$, $|01\rangle \mapsto |01\rangle$, $|10\rangle \mapsto |11\rangle$, and $|11\rangle \mapsto |10\rangle$. After this bilateral CNOT operation, both target qubits (3 and 4) are measured in the logical basis. If the outcomes of Alice's and Bob's measurement are the same, they keep the source pair, otherwise it is discarded. The fidelity F' of the remaining pair turns out to be larger than the initial fidelity F provided that $1/2 < F < 1$. Another π

rotation about the y axis again exchanges $|\Psi^-\rangle$ and $|\Phi^+\rangle$ components. Therefore, iterating the scheme can bring the fidelity arbitrarily close to 1, resulting in a maximally entangled Bell state. Since the state after one purification round is not a Werner state, the last step is necessary as a prerequisite for the twirl in the subsequent round.

The difference in the Deutsch *et al.* [7] protocol (DEJMPS) is that it works generally on Bell-diagonal states and therefore does not need the twirl to come back to Werner form. A purification round begins with Alice performing the single-qubit gate

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle), \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|1\rangle - i|0\rangle), \quad (2)$$

on both of her qubits and Bob the inverse operation. As in the BBPSSW protocol, a bilateral CNOT and the measurement of the target pair follow, keeping the source qubits only if the outcomes are equal. If the initial $|\Phi^+\rangle$ component is larger than $1/2$, the states can be purified to a pure $|\Phi^+\rangle$ state, but in a more efficient way than in [6].

Spin Qubits. The CNOT gate is not directly generated by the typical interaction between spin qubits in gate-defined quantum dots, where the exchange interaction can be described by a Heisenberg Hamiltonian [14, 27]. Two interaction pulses and additional single-qubit operations on both qubits are necessary to construct the CNOT gate [14]. However, since single-spin rotations are much slower than spin-spin exchange interactions, such an implementation is challenging. We therefore construct a purification protocol requiring only a single two-qubit operation each for Alice and Bob, which is directly generated from the Heisenberg Hamiltonian describing the exchange interaction between the spins of two electrons confined to adjacent gate-defined QDs [14, 27],

$$H_{ij}(t) = \frac{1}{4}J(t)\sigma_i \cdot \sigma_j = J(t)\left(\frac{1}{4}\mathbb{1} - P_{\Psi^-}\right), \quad (3)$$

where σ_i is the Pauli spin operator of the electron in QD i , $P_{\Psi^-} = |\Psi^-\rangle\langle\Psi^-|$, and $J(t)$ is the exchange energy between the two electrons that can be tuned by changing appropriate gate voltages, and hence can depend on time t . The two possible spin orientations of an electron define the logical states $|0\rangle \equiv |\uparrow\rangle$ and $|1\rangle \equiv |\downarrow\rangle$.

The time evolution U generated by (3) is given by $U_{ij}(\alpha) = \exp[-i \int_0^\tau dt H_{ij}(t)] = e^{-i\alpha/4}(\mathbb{1} + (e^{i\alpha} - 1)P_{\Psi^-})$ where we set $\hbar = 1$, assume a pulsed exchange coupling of duration τ , and refer to $\alpha = \int_0^\tau dt J(t)$ as the pulse area. For each value of α , a specific two-qubit gate is generated, especially the entangling $\sqrt{\text{SWAP}}$ gate for $\alpha = \pi/2$ [14, 27], $U_{\sqrt{\text{SWAP}}} = e^{i\pi/8}U_{ij}(\pi/2)$, which together with arbitrary single-qubit operations forms a universal set of quantum gates [14, 28], or the SWAP operation for $\alpha = \pi$, $U_{\text{SWAP}} = (U_{\sqrt{\text{SWAP}}})^2 = e^{i\pi/4}U_{ij}(\pi)$, whose action is to interchange the states of the qubits [29].

The CNOT can be obtained by the sequence [14] $U_{\text{CNOT}} = e^{-i\pi/2} e^{-i\pi\sigma_2^z/4} e^{i\pi\sigma_1^z/4} e^{-i\pi\sigma_2^z/4} U_{\sqrt{\text{SWAP}}} e^{i\pi\sigma_1^z/2} U_{\sqrt{\text{SWAP}}} e^{i\pi\sigma_2^z/4}$, requiring two $\sqrt{\text{SWAP}}$ and several single-qubit gates.

Purification with the Exchange Interaction. We now introduce a purification protocol, that only makes use of a single activation of the Heisenberg interaction (3). The protocol has the same structure as existing recurrence protocols [6], the crucial difference being that the bilateral operation is *asymmetric*, meaning one has to apply *different* two-qubit gates. The two parties Alice and Bob each start with a copy of the state ρ_F , with $\rho = \rho_F \otimes \rho_F$, which can be generated as shown above. Then, Alice and Bob each activate the exchange interaction between their two qubits with specific pulse areas α and β respectively (Fig. 1), i.e. they apply the unitary transformation

$$U(\alpha, \beta) = U_{13}(\alpha) \otimes U_{24}(\beta), \quad (4)$$

$$F'(F, \alpha, \beta) = \frac{(4F-1)(4F+5) \cos \alpha \cos \beta - (4F-1)(8F+1) \sin \alpha \sin \beta + 8F(4F+1) + 5}{6(4F-1) \cos \alpha \cos \beta - 2(4F-1)^2 \sin \alpha \sin \beta + 6(4F+5)}, \quad (5)$$

which is the main result of this paper.

To show the feasibility of the protocol, the three fixed points of the map (5) can be found analytically. Except for the case $\alpha = n\pi$, $\beta = m\pi$, and $\alpha - \beta = 2\pi k$ (n, m, k integers), where $F' \equiv F$, a constant fixed point is given by $F_c = 1/4$. The values of the two remaining (possibly complex) fixed points F_{\min} and F_{\max} depend on α and β , as illustrated in Fig. 2 within the physically relevant regime $1/2 \leq F_{\min} \leq F_{\max} \leq 1$. While F_{\max} and F_c are attractive, F_{\min} is repulsive. Thus, if the qubit pairs have

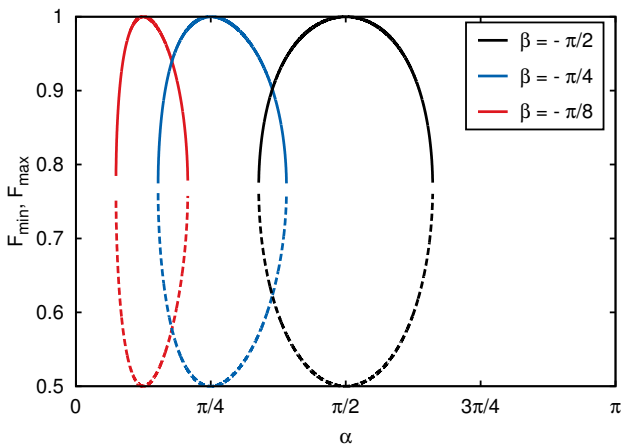


FIG. 2. The minimum required initial fidelity F_{\min} (dashed line) for the entanglement purification to work and the maximally attainable fidelity F_{\max} (solid line) when iteratively applying the purification protocol generating the map (5) as a function of the pulse area α , for different pulse areas β .

where Alice holds qubits 1 and 3, Bob qubits 2 and 4. This transforms the initial state ρ into $U(\alpha, \beta)\rho U(\alpha, \beta)^\dagger$. After this unitary transformation, the two parties continue as in the BBPSSW protocol. The target qubits 3 and 4 are measured in the z basis and the results are communicated via a classical channel. If the spins point in the same direction, Alice and Bob keep qubits 1 and 2 (source pair), otherwise the state is discarded.

We find the fidelity $F' = \langle \Phi^+ | \rho' | \Phi^+ \rangle$ of the postselected source state ρ' after the described procedure to be

an initial fidelity $F > F_{\min} \geq 1/2$, iterative application of the described scheme can purify them up to a fidelity F_{\max} .

Optimal Purification. The minimal and maximal values of the fixed points $F_{\min} = 1/2$ and $F_{\max} = 1$ are obtained in the case $\beta = -\alpha$. This implies that in principle maximally entangled states can be created using our protocol if Alice and Bob perform mutually inverse operations. This could be achieved either using ferro- and antiferromagnetic exchange $J_A > 0$, $J_B < 0$, or vice versa, or in the case of equal coupling types, using the fact that the propagator U_{ij} is 2π periodic (omitting overall phases), with, e.g., $0 < \alpha < \pi$ and $\beta = 2\pi - \alpha > 0$. The fidelity is then given by

$$F'(F, \alpha, -\alpha) = \frac{1}{2} + \frac{3 - 12F^2}{(F-1)(4F-1) \cos(2\alpha) - F(4F+7) - 7}, \quad (6)$$

and has its maximum in the optimal case $\alpha = \pi/2$,

$$F' \left(F, \frac{\pi}{2} + 2\pi n, -\frac{\pi}{2} + 2\pi m \right) = \frac{16F^2 + F + 1}{8F^2 + 2F + 8}. \quad (7)$$

The result Eq. (6) is plotted in Fig. 3(a) for different values of α . The optimal value is therefore achieved if Alice applies a $\sqrt{\text{SWAP}}$ gate to her qubits and Bob performs the inverse $\sqrt{\text{SWAP}}$ gate, $\sqrt{\text{SWAP}}^{-1}$. The square of $\sqrt{\text{SWAP}}^{-1}$ is also the SWAP operation and it can be understood as another root of SWAP.

The described protocol can be slightly improved in terms of resources needed to achieve a specific fidelity. In analogy to the DEJMPS protocol, Alice can begin each

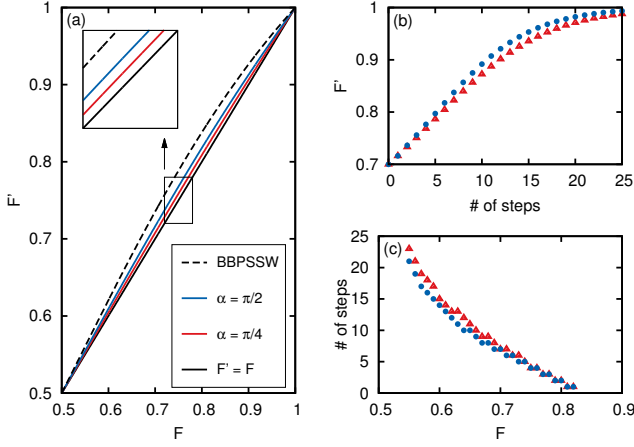


FIG. 3. (a) The fidelity F' as a function of the initial fidelity F , shown for different pulse areas α and compared to the BBPSSW protocol. (b) Stepwise fidelity increase for an initial fidelity $F = 0.7$ and (c) number of steps needed to achieve a fidelity $F' > 0.99$ starting from qubit pairs with a fidelity F ; shown for the described protocol (triangles) in the optimal case (7) and in the more efficient way in analogy to the DEJMPS protocol (dots).

purification step with the local operations (2) (and Bob with the inverse) and the bilateral CNOT is replaced by the asymmetric operation described above, to increase the gain in fidelity (Fig. 3(b)) and therefore reduce the number of purification steps (Fig. 3(c)). Furthermore, one can see from Fig. 2 that the robustness of our scheme is largest in the case $\alpha = -\beta = \pi/2$, since deviations from perfectly applied operations have the least effect on the values of F_{\min} and F_{\max} . If Alice applies a rectangular pulse with an exchange interaction of $J = 1 \mu\text{eV}$ [30], the deviation $\Delta\tau$ from the optimal case must not exceed 100 ps to still achieve a maximum fidelity of 0.99, assuming Bob generates a perfect pulse. Such accuracies can be obtained experimentally [30].

Purification with the XY Interaction. We briefly discuss our approach for entanglement purification and applying an asymmetric bilateral operation for the case of anisotropic XY-type qubit interactions, $H_{XY}(t) = \frac{1}{4}J(t)(\sigma_1^x\sigma_2^x + \sigma_1^y\sigma_2^y)$. This kind of interaction appears, e.g., in all-optical cavity-coupled QD electron spins [19] or superconducting qubits [18]. The Hamiltonian $H_{XY}(t)$ generates the iSWAP gate, $|\uparrow\uparrow\rangle \mapsto |\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle \mapsto i|\downarrow\uparrow\rangle$, $|\downarrow\uparrow\rangle \mapsto i|\uparrow\downarrow\rangle$, $|\downarrow\downarrow\rangle \mapsto |\downarrow\downarrow\rangle$, for a pulse area $\int_0^\tau dt' J(t') = -\pi$. Following the above scheme, applying interactions with different pulse areas α and β on Alice's and Bob's qubits, the fidelity F' after the protocol is

$$F'(F, \alpha, \beta) = \frac{(12F - 3) \cos \alpha \cos \beta - (4F - 1)^2 \sin \alpha \sin \beta + 4(8F^2 + 2F - 1) \cos \frac{\alpha + \beta}{2} + 4F(4F + 1) + 7}{6(4F - 1) \cos \alpha \cos \beta - 2(4F - 1)^2 \sin \alpha \sin \beta + 6(4F + 5)}. \quad (8)$$

In the case $\alpha = -\beta$, the result coincides with (6) and therefore is maximal for $\alpha = \pi/2$. The optimal bilateral two-qubit gates in the case of the XY Hamiltonian are square roots of iSWAP.

Conclusions. We have presented an entanglement purification scheme, in which the bilateral two-qubit operation is directly generated from the one-time activation of a Heisenberg-type spin-spin interaction. In general we could show that an asymmetric unitary evolution of Alice's and Bob's qubits, respectively, can lead to an increased fidelity of one of the shared qubit pairs with respect to $|\Phi^+\rangle$ if the initial fidelity was larger than a given minimal value. In the special case where Alice and Bob apply inverse operations, the maximally obtainable fidelity by iterative application of our protocol is $F = 1$, i.e., in principle maximally entangled states can be generated. We found that the optimal case is when the two communicating parties apply the $\sqrt{\text{SWAP}}$ and the $\sqrt{\text{SWAP}}^{-1}$ gates locally on their qubits.

Since the coupling of electron spins in gate-controlled QDs is well described by an exchange interaction of Heisenberg type, the protocol is particularly suitable for

spin qubits. In terms of operation times, the presented protocol is much faster than protocols based on CNOT applied to spin qubits. The reason is that single-qubit gates needed in constructing the CNOT need operation times on the order of 100 ns [31] whereas the $\sqrt{\text{SWAP}}$ can be generated two orders of magnitude faster in about 0.2 ns [30]. Therefore, besides the smaller error-proneness due to the smaller number of gate operations, a much faster iteration of the protocol is possible. In addition, we showed that our purification method of applying an asymmetric bilateral operation works as well for qubits coupled via a XY-type interaction and is therefore suitable for cavity-coupled spin qubits and superconducting qubits.

Acknowledgements. We acknowledge funding from the DFG within SFB 767 and from the BMBF under the program QuaHL-Rep.

* adrian.auer@uni-konstanz.de

[1] D. Bouwmeester, A. K. Ekert, and A. Zeilinger, *The*

Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation (Springer New York, 2001).

- [2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [3] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
- [4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore* (1984) pp. 175–179.
- [5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
- [7] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
- [8] W. Dür and H. J. Briegel, Rep. Prog. Phys. **70**, 1381 (2007).
- [9] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
- [10] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
- [11] H. J. Kimble, Nature **453**, 1023 (2008).
- [12] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, and R. J. Young, Eur. Phys. J. D **58**, 1 (2010).
- [13] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
- [14] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).
- [15] F. H. L. Koppens, K. C. Nowack, and L. M. K. Vandersypen, Phys. Rev. Lett. **100**, 236802 (2008).
- [16] R. Hanson, L. P. Kouwenhoven, J. R. Petta, S. Tarucha, and L. M. K. Vandersypen, Rev. Mod. Phys. **79**, 1217 (2007).
- [17] J. Berezovsky, M. H. Mikkelsen, N. G. Stoltz, L. A. Coldren, and D. D. Awschalom, Science **320**, 349 (2008).
- [18] Y. Makhlin, G. Schön, and A. Shnirman, Rev. Mod. Phys. **73**, 357 (2001).
- [19] A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, Phys. Rev. Lett. **83**, 4204 (1999).
- [20] T. Tanamoto, K. Maruyama, Y.-x. Liu, X. Hu, and F. Nori, Phys. Rev. A **78**, 062313 (2008).
- [21] K. Maruyama and F. Nori, Phys. Rev. A **78**, 022312 (2008).
- [22] D. Gonça and P. van Loock, Phys. Rev. A **84**, 042303 (2011).
- [23] D. Gonça and P. van Loock, Phys. Rev. A **86**, 052312 (2012).
- [24] J. M. Taylor, W. Dür, P. Zoller, A. Yacoby, C. M. Marcus, and M. D. Lukin, Phys. Rev. Lett. **94**, 236803 (2005).
- [25] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [26] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [27] G. Burkard, D. Loss, and D. P. DiVincenzo, Phys. Rev. B **59**, 2070 (1999).
- [28] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
- [29] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
- [30] J. R. Petta, A. C. Johnson, J. M. Taylor, E. A. Laird, A. Yacoby, M. D. Lukin, C. M. Marcus, M. P. Hanson, and A. C. Gossard, Science **309**, 2180 (2005), <http://www.sciencemag.org/content/309/5744/2180.full.pdf>.
- [31] K. C. Nowack, F. H. L. Koppens, Y. V. Nazarov, and L. M. K. Vandersypen, Science **318**, 1430 (2007), <http://www.sciencemag.org/content/318/5855/1430.full.pdf>.